Amendments to the Claims

Please amend the claims as indicated in the following listing of claims. This listing replaces all prior listings of the claims.

1. (Currently Amended) A method in a data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, comprising:

receiving a request from a user for a digital certificate, the request including an encryption key associated with the user; ~~and~~

encrypting the user's encryption key with a first archival key;

storing the encrypted user's encryption key in a database under the control of a first entity separate from the certificate authority;

providing an indication of proof of storing the encrypted user's encryption key, wherein the indication of proof is signed with a second archival key;

verifying the signed indication of proof based on the first archival key; and

providing the request to the certificate authority based on the verification of the signed indication of proof.

~~receiving an indication of proof of archival of the user's encryption key associated with the request, wherein the user's encryption key is archived under control of an entity other than the certificate authority.~~

2. (Currently Amended) The method of claim 1, further comprising the step of sending a digital certificate from the certificate authority to the user in response to the certificate authority receiving request ~~associated with the user in response to the received request and indication of proof of archival~~.

3. (Currently Amended) The method of claim 1, wherein encrypting the user's encryption key with a first archival key is performed by the first entity.

~~further comprising the step of receiving the user's encryption key~~.

4. (Currently Amended) The method of claim 3, further comprising:

encrypting the request with a transport key; and

sending the transport encrypted request to the first entity.

~~wherein the encryption key is encrypted during transmission, and wherein the method further comprises the step of decrypting the encrypted encryption key.~~

5. (Currently Amended) The method of claim ~~4~~3, further comprising:

decrypting, by the first entity, the transport encrypted request.

~~wherein the encryption key is the user's private key.~~

6. (Currently Amended) The method of claim 4, wherein the ~~data processing system comprises~~ first entity is a data recovery manager that receives and manages archiving of the encryption key, and wherein the transport key ~~encryption key is encrypted during transmission using~~ the data recovery manager's public transport key.

7. (Currently Amended) The method of claim ~~1~~ 6, wherein the second archival key is a data recovery manager private key.

~~indication of proof of archival is digitally signed, and wherein the method further comprises the step of verifying a digital signature on the indication of proof of archival.~~

8. (Currently Amended) The method of claim ~~7~~ 1, wherein providing an indication of proof of storing the encrypted user's encryption key includes signing, by the first entity, the indication of proof, and wherein verifying the signed indication of proof is performed by a second entity separate from the first entity and the certificate authority.

~~the data processing system includes a data recovery manager that receives and manages archiving of the encryption key, and wherein the indication of proof of archival is digitally signed by the data recovery manager.~~

9. (Original) The method of claim 1, wherein the user's encryption key is archived under control of the user.

10. (Currently Amended) A method in a data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, comprising:

digitally signing an indication of proof of archival of an encryption key for the user in a database under the control of an entity separate from the certificate authority;

verifying the digitally signed indication of proof;

sending a request for a digital certificate based on the verifying~~, the request having an indication of proof of archival of an encryption key for the user~~; and

receiving a digital certificate in response to the request.

11. (Canceled).

12. (Currently Amended) A method in a data processing system for archiving an encryption key by ~~an~~ a first entity other than a certificate authority, comprising:

receiving an encryption key for archiving;

archiving the received encryption key;

creating an indication of proof of archival of the received encryption key; and

~~sending~~ providing the indication of proof of archival to a second entity that verifies the indication of proof and provides a request for a digital certificate from the certificate authority based on a verified indication of proof.

13. (Original) The method of claim 12, further comprising the step of digitally signing the indication proof of archival.

14. (Currently Amended) The method of claim 13, wherein the archiving step further comprises step archiving the received encryption under control of a user.

15. (Currently Amended) A data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, comprising:

a memory having program instructions; and

a processor configured to execute the program instructions to receive a request from a user for a digital certificate, ~~and~~ receive an indication of proof of archival of the user's encryption key associated with the request, verify the indication of proof, wherein the user's encryption key is archived under control of an entity other than the certificate authority, and provide the request to the certificate authority based on the verification of the indication of proof.

16. (Currently Amended) A data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, comprising:

a memory having program instructions; and

a processor configured to execute the program instructions to send a request for a digital certificate, the request having ~~an~~ a verified indication of proof of archival of an encryption key for the user in an entity separate from the certificate authority , and receive a digital certificate in response to the request.

17. (Currently Amended) A data processing system for archiving an encryption key by an entity other than a certificate authority, comprising:

a memory having program instructions; and

a processor configured to execute the program instructions to receive an encryption key for archiving, archive the received encryption key, create an indication of proof of archival of the received encryption key, and send the indication of proof of archival to an entity that provides a request for a digital certificate to the certificate authority based on a verification of the indication of proof of archival.

18. (Original) A data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key under control of an entity other than the certificate authority, comprising:

a registration manager configured to receive a digital certificate request including a user's encryption key, send the user's encryption key, and in response receive an indication of proof of archival;

a data recovery manager configured to receive the user's encryption key, send the user's encryption key to a database controlled by an entity other than the certificate authority for archiving, create an indication of proof archival and send the indication of proof of archival;

a certificate authority configured to issue a digital certificate when it is determined that an indication proof of archival was received; and

a database, under control of an entity other than the certificate authority, configured to receive and archive the user's encryption key.

19. (Currently Amended) A computer-readable medium containing instructions for controlling a data processing system to perform a method for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, the method comprising the steps of:

receiving a request including a user's encryption key from a user for a digital certificate; ~~and~~

receiving an indication of proof of archival of the user's encryption key associated with the request, wherein the user's encryption key is archived under control of an entity other than the certificate authority;

verifying the indication of proof; and

receiving a digital certificate from the certificate authority based on the verified indication of proof,

wherein the data processing system comprises a data recovery manager separate from the certificate authority that receives and manages archiving of the encryption key, and wherein the user's encryption key is encrypted during transmission from the user using the data recovery manager's public transport key.

20. (Original) The computer-readable medium of claim 19, wherein the method further comprises the step of sending a digital certificate associated with the user in response to the received request and indication of proof of archival.

21. (Currently Amended) The computer-readable medium of claim 19, wherein the data processing system includes a registration manager separate from the certificate authority that sends the encrypted user's encryption key to the data recovery manager.

~~the method further comprises the step of receiving the user's encryption key.~~

22. (Canceled)

23. (Canceled)

24. (Canceled)

25. (Original) The computer-readable medium of claim 19, wherein the indication of proof of archival is digitally signed, and wherein the method further comprises the step of verifying a digital signature on the indication of proof of archival.

26. (Currently Amended) The computer-readable medium of claim 25, wherein the ~~data processing system includes a~~ data recovery manager ~~that receives and manages archiving of the encryption key, and wherein the indication of~~ digitally signs the proof of archival ~~is digitally signed by the data recovery manager~~.

27. (Original) The computer-readable medium of claim 19, wherein the user's encryption key is archived under control of the user.

28. (Currently Amended) A computer-readable medium containing instructions for controlling a data processing system to perform a method for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, the method comprising the steps of:

digitally signing an indication of proof of archival of an encryption key for the user in a database under the control of an entity separate from the certificate authority;

verifying the digitally signed indication of proof;

sending a request for a digital certificate based on the verified digitally signed indication of proof~~, the request having an indication of proof of archival of an encryption key for the user~~; and

receiving a digital certificate in response to the request.

29. (Canceled)

30. (Currently Amended) A computer-readable medium containing instructions for controlling a data processing system to perform a method for archiving an encryption key by ~~an~~ first entity other than a certificate authority, the method comprising the steps of:

receiving an encryption key for archiving;

archiving the received encryption key;

creating an indication of proof of archival of the received encryption key; and

~~sending~~ providing the indication of proof of archival to a second entity that provides a request for a digital certificate from the certificate authority based on a verification of the indication of proof.

31. (Original) The computer-readable medium of claim 30, wherein the method further comprises the step of digitally signing the indication proof of archival.

32. (Original) The computer-readable medium of claim 31, wherein the archiving step further comprises the step of archiving the received encryption key under control of a user.

33. (Currently Amended) A data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, comprising:

means for receiving a request from a user for a digital certificate, the request including an encryption key associated with the user; ~~and~~

means for encrypting the user's encryption key with a first archival key;

means for storing the encrypted user's encryption key in a database under the control of a first entity separate from the certificate authority;

means for providing an indication of proof of storing the encrypted user's encryption key, wherein the indication of proof is signed with a second archival key;

means for verifying the signed indication of proof based on the first archival key; and

means for providing the request to the certificate authority based on the verification of the signed indication of proof.

~~means for receiving a request from a user for a digital certificate; and~~

~~means for receiving an indication of proof of archival of the user's encryption key associated with the request, wherein the user's encryption key is archived under control of an entity other than the certificate authority.~~